REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed December 13. 2007. Through this response, claims 1, 24, 38, 55, 69, 77, 83, 92, 100, 105, 110, 115, and 120 have been amended. Reconsideration and allowance of the application and pending claims 1-124 are respectfully requested.

I. Claim Rejections - 35 U.S.C. § 112, First Paragraph

Claims 1, 24, 38, 55, 69, 77, 83, 92, 100, 105, 110, 115 and 120 have been rejected under 35 U.S.C. § 112, first paragraph, as allegedly lacking support in the specification for the previously filed claim amendments. Applicants have deleted the language pertaining to "decryption block." In that those objections are believed to have been rendered moot, Applicants respectfully request that the rejection of these claims under 35 U.S.C. § 112, first paragraph, be withdrawn.

II. Claim Rejections - 35 U.S.C. § 103(a)

A. Statement of the Rejection

Claims 1-124 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Rabowsky* ("*Rabowsky*," U.S. Pat. No. 6,141,530) in view of *Bartholet et al.* ("*Bartholet*," U.S. Pub. No. 2002/0114453). Applicants respectfully traverse this rejection.

B. Discussion of the Rejection

The M.P.E.P. § 2100-116 states:

> Office policy is to follow *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), in the consideration and determination of obviousness under 35 U.S.C. 103. . . the four factual inquires enunciated therein as a background for determining obviousness are as follows:

(A) Determining the scope and contents of the prior art;
(B) Ascertaining the differences between the prior art and the claims in issue;
(C) Resolving the level of ordinary skill in the pertinent art; and
(D) Evaluating evidence of secondary considerations.

In the present case, it is respectfully submitted that a *prima facie* case for obviousness is not established using the art of record.

Independent Claim 1

Claim 1 recites:

> 1. A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver;
>
> applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet; and
>
> applying to the second ciphertext packet a second cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 1. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related

> protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 1 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 2-23 are allowable as a matter of law for at least the reason that the dependent claims 2-23 contain all elements of their respective base claim. See, *e.g.*, *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

Independent Claim 24

Claim 24 recites:

> 24. A method for securely providing in a subscriber network encrypted programming, which is received at a receiver at a subscriber location, the encrypted programming includes a plurality of ciphertext packets, and wherein the subscriber network includes a headend for distributing the encrypted programming and a plurality of receivers including the receiver at the subscriber location, at the headend the method comprising the steps of:
>
> applying to a cleartext packet a first cryptographic algorithm to convert the cleartext packet to a first ciphertext packet;
>
> transmitting the first ciphertext packet to the receiver; and
>
> at the receiver the method comprising the steps of:
>
> receiving the first ciphertext packet;
>
> applying to the first ciphertext packet a second cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet; and
>
> applying to the second ciphertext packet a third cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 24. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> <u>The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream</u> and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, <u>and a reverse channel which provides data back to the headend system from the theaters</u>.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a

> previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 24 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 25-37 are allowable as a matter of law.

Independent Claim 38

Claim 38 recites:

> 38. A receiver in a subscriber network that receives encrypted programming, from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first ciphertext packet of the encrypted programming;
>
> a key generator adapted to generate a plurality of encryption keys; and
>
> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm at least twice using at least one encryption key and the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 38. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> <u>The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system</u>, <u>receiver-decoders which receive the radio frequency bit stream</u> and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, <u>and a reverse channel which provides data back to the headend system from the theaters</u>.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key

> by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 38 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 39-54 are allowable as a matter of law.

Independent Claim 55

Claim 55 recites:

> 55. A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver; and
>
> applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 55. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the

> cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys… substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved…By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users…the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random

> memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 55 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 56-68 are allowable as a matter of law.

Independent Claim 69

Claim 69 recites:

> 69. A method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto, at the headend the method comprising the steps of:
>
> receiving a first ciphertext packet;
>
> applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet;
>
> transmitting the second ciphertext packet; and
>
> at the receiver the method comprising the steps of:
>
> receiving the second ciphertext packet having multiple layers of encryption thereon; and
>
> applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 69. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities…Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.

> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 69 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 70-76 are allowable as a matter of law.

Independent Claim 77

Claim 77 recites:

> 77. The method for securely providing a subscriber of a subscriber network with an encrypted program, wherein the encrypted program includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving a first ciphertext packet of the encrypted program;
>
> applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet; and
>
> transmitting the second ciphertext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 77. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> <u>The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system</u>, <u>receiver-decoders which receive the radio frequency bit stream</u> and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, <u>and a reverse channel which provides data back to the headend system from the theaters</u>.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other

> in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the

reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 77 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 78-82 are allowable as a matter of law.

Independent Claim 83

Claim 83 recites:

> 83. A receiver in a subscriber network that receives encrypted programming from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon;
>
> a key generator adapted to generate an encryption key; and

> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 83. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.

> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 83 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 84-91 are allowable as a matter of law.

Independent Claim 92

Claim 92 recites:

> 92. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using a first key;
>
> generating a second and third key;
>
> applying to the first ciphertext packet a second cryptographic algorithm with the second key to convert the first ciphertext packet to a

> second ciphertext packet having a second layer of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet; and
>
> applying to the second ciphertext packet a third cryptographic algorithm with the third key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 92. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.

> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 92 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 93-99 are allowable as a matter of law.

Independent Claim 100

Claim 100 recites:

> 100. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first ciphertext of the encrypted programming, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using a first key;
>
> a key generator adapted to generate a plurality of keys including a second key and a third key;

> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet, without first converting the first ciphertext packet received from the headend to a cleartext packet, using a second cryptographic algorithm and the second key and thereafter to convert the second ciphertext packet to a third ciphertext packet, without first converting the second ciphertext packet to a cleartext packet, using a third cryptographic algorithm and the third key; and
>
> a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second and third keys.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 100. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky.* According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> <u>The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system</u>, <u>receiver-decoders which receive the radio frequency bit stream</u> and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as

> authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be

> transferred between users…the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the

reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 100 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 101-104 are allowable as a matter of law.

Independent Claim 105

Claim 105 recites:

> 105. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, the second key and the third key;

> generating a fourth key;
>
> applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet; and
>
> applying to the second ciphertext packet a third cryptographic algorithm with the fourth key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 105. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> <u>The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system</u>, <u>receiver-decoders which receive the radio frequency bit stream</u> and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, <u>and a reverse channel which provides data back to the headend system from the theaters</u>.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of <u>key distribution for data transfer or storage, results in either unintentional disclosure of the keys</u> to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, <u>complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost</u> of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an <u>innovative alternative to conventional methods of key management</u>. In particular, the inventions facilitate an infrastructure within which <u>data is secured using in situ generated encryption and decryption keys</u>... <u>substantially eliminating any need for key distribution</u> and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, <u>no encryption/decryption keys need be transferred between users</u>...the users may communicate with each other

> in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the

reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 105 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 106-109 are allowable as a matter of law.

Independent Claim 110

Claim 110 recites:

> 110. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, a second key and a third key;

> a key generator adapted to generate a fourth key;
>
> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet and thereafter to convert the second ciphertext packet to a third ciphertext packet using a third cryptographic algorithm and the fourth key without first converting the second ciphertext packet to a cleartext packet; and
>
> a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second, third and fourth keys.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 110. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> <u>The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream</u> and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as

> authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be

> transferred between users…the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the

reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 110 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 111-114 are allowable as a matter of law.

Independent Claim 115

Claim 115 recites:

> 115. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key and a second key, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;
>
> generating a third key; and
>
> applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 115. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities…Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the

> cost of maintaining a cryptographic communication or data storage system.
>
> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random

> memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 115 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 116-119 are allowable as a matter of law.

Independent Claim 120

Claim 120 recites:

> 120. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;
>
> a key generator adapted to generate a third key;
>
> a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting the first ciphertext packet received from the headend to a cleartext packet; and
>
> a storage device in communication with the cryptographic device adapted to store the second ciphertext packet and the first, second and third keys.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established for the rejection to claim 120. The Office Action (page 5) alleges the following with regard to the combination of *Rabowsky* and *Bartholet*:

> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the multi-layer encryption scheme taught by Bartholet in the system of Rabowsky to further encrypt the incoming ciphertext packets one or more times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack.

Applicants respectfully disagree that it would have been obvious to combine *Bartholet* with *Rabowsky*. According to well-established case law, "[I]t is improper to combine references where the references teach away from their combination." *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). With regard to application of the law to the current rejection, Applicants respectfully note that *Rakowsky* (see, e.g., col. 1, lines 9-10) appears to be directed to "secure electronic delivery of motion pictures in digital format." According to *Rakowsky* (see, e.g., col. 1, line 61 – col. 2, line 4), one system arrangement comprises the following features (emphasis added):

> The theater system comprises transmission line interfaces at theaters designated to receive cinema and data files from the headend system, receiver-decoders which receive the radio frequency bit stream and produce decoded cinema and data files at baseband, storage playback systems which stores cinema and data files until needed, secure projector systems which playback cinema files, an automation/scheduling system which directs playback of cinema files in the secure projector systems as authorized by the management system, and a reverse channel which provides data back to the headend system from the theaters.

In other words, *Rakowsky* appears *arguendo* to disclose a headend-receiver system. Further, Figure 2 of *Rakowsky* shows a conditional access module 72 residing in the theater referenced above, and column 9, line 65 – col. 10, line 10 provides the following explanation with regard to a conditional access module residing therein:

> A CAM receives EMM and ECM data from the headend, verifies the authenticity of the data, compares the data with stored information, for example, in a Smart Card, and, if validity is established, generates a key word necessary to enable the decryptor. In a preferred version of the present invention, the key word is generated on a packet by packet basis. In this case, each location which has an encryptor and/or a decryptor has an associated receiver-decoder and a CAM. These locations include the Secure Projector System, the Speaker System, and the User Data Channel. The key word is transferred to the encryptor/decryptor in a secure environment. For example, removal of the Smart Card or the CAM from the receiver-decoder disables the receiver-decoder.

Clearly from above cited section of *Rakowsky*, the headend appears *arguendo* to provide or distribute entitlement information (e.g., headend-provided keys) to the CAM of the theater, according to conventional methods such as Triple DES (e.g., as referenced in column 4).

In contrast, *Bartholet* teaches away from such systems and methods, as highlighted below in the referenced paragraph "portions" from *Bartholet* (emphasis added):

> [0008] Often, the process of key distribution for data transfer or storage, results in either unintentional disclosure of the keys to third parties or interception/extraction of the keys or key material by unauthorized entities...Additionally, complex key management infrastructures that change and distribute keys on a frequent basis increase logistics and the cost of maintaining a cryptographic communication or data storage system.

> [0009] The inventions described in the referenced patents enhance significantly the security of cryptographic systems by applying an innovative alternative to conventional methods of key management. In particular, the inventions facilitate an infrastructure within which data is secured using in situ generated encryption and decryption keys... substantially eliminating any need for key distribution and capable of keeping the keys unknown to all parties involved...By using the in situ pseudo-random key generators, no encryption/decryption keys need be transferred between users...the users may communicate with each other in encryption mode without ever having to transmit the keys over the communication lines.
>
> [0015] No conventional key management infrastructure is required for cryptographic data transmission and storage of files and data, since all the keys are internally generated by the in situ key generators for use in the authorized network;

Evidently, *Bartholet* is not only teaching a system that appears to address the perceived shortcomings of systems like *Rakowsky*, but also operates in a completely different manner than *Rakowsky*. Paragraph [0032] from *Bartholet* provides as follows (emphasis added):

> [0032] In the case of incoming encrypted data destined for decryption and display on a computer terminal (Operating Mode A1 of FIG. 4), the encrypted data from an External Terminal block 103 is transmitted via a public or private Network 104 to the I/O & Protocols block 105. For a given time or event, the Gateway and Storage PKG 106 preferably generates the same keys as those generated by a PKG in an external terminal that is sending the encrypted data to block 105. The generated keys are sent to the Data Decryptors, blocks 107, 108, and 109; that is, a previous key period--Data Decryptor Key A, block 107, a present key period--Data Decryptor Key B, block 108, and the next key period--Data Decryptor Key C, block 109. With all three decryptors working in parallel, preferably one of the three will succeed in decrypting the incoming data. This is known on a packet-by-packet basis by a portion of a known header or flag information being properly decrypted with the correct key by only one of the three decryptors. This known information in the data may come from added overhead put into the data during the encryption process or may be from a header already available from other network requirements such as a TCP or IP address or other such network related protocols. All three decryptor outputs are sent to the Data Processor & Boundary Counter block 110, which in turn passes only the correctly decrypted packets to the Storage Controller block 111.). The data is then passed on to the Terminal block 112 for display. In all operating modes described for FIG. 1, the Rate Buffer block 117 serves as a random memory device for data overflow, to cover any mismatches between data rates for storage, for communication or for display.

In other words, it is the local gateway 106 (local to storage) that distributes the keys, not the external device 103 over a communications network 104. Such an arrangement for the distribution of keys teaches away from *Rakowsky*'s disclosed systems and methods, and hence, the references are not properly combinable. Accordingly, for at least the reason that the proposed combination of *Rabowsky* in view of *Bartholet* is improper, and because each individual reference alone fails to disclose, teach, or suggest all of the claim features, Applicants respectfully request that the rejection be withdrawn.

Additionally, Applicants respectfully submit that there exists no suggestion or motivation to combine *Rabowsky* and *Bartholet*. It has been well established that teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). *Rabowsky* does not teach multiple tiers of encryption at the theater. Although the Office Action proffers a motivation ("to raise the cost of the known-plaintext attack"), even assuming *arguendo* that raising the cost is a possibility (admission of which is neither expressed nor implied), Applicants respectfully submit that one having ordinary skill in the art would reasonably expect an increased cost of implementing multi-tiered functionality that might offset or even overcome any perceived benefits to implementation. Accordingly, for this additional and separate reason, Applicants respectfully submit that a *prima facie* case of obviousness is not established, and respectfully request that the rejection be withdrawn.

Because independent claim 120 is allowable over *Rabowsky* in view of *Bartholet*, dependent claims 121-124 are allowable as a matter of law.

In summary, it is Applicants' position that a *prima facie* for obviousness has not been made against Applicants' claims. Therefore, it is respectfully submitted that each of these claims is patentable over the art of record and that the rejection of these claims should be withdrawn.

CONCLUSION

Applicants respectfully submit that Applicants' pending claims are in condition for allowance. Any other statements in the Office Action that are not explicitly addressed herein are not intended to be admitted. In addition, any and all findings of inherency are traversed as not having been shown to be necessarily present. Furthermore, any and all findings of well-known art and official notice, and similarly interpreted statements, should not be considered well known since the Office Action does not include specific factual findings predicated on sound technical and scientific reasoning to support such conclusions. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,

/dr/
David Rodack
Registration No. 47,034

**THOMAS, KAYDEN,
HORSTEMEYER & RISLEY, L.L.P.**
Suite 1500
600 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500